Infocentricity and Beyond

How the Intelligence Community Can Survive the Challenges of Emerging Technologies, Shrinking Budgets, and Growing Suspicions

Diane Mezzanotte
Strategic Force Planning Paper
NSDM/Fort Meade
April 2000

Word count: 4861

Diane L Mezzanotte
10 May 2000

REPORT DOCUMENTATION PAGE

1. Report Security Classification:	UNCLASSIFIED
2. Security Classification Authority:	S3 Classif. Advisory Officer, NSA (E. Moken)
3. Declassification/Downgrading Schedule:	N/A
4. Distribution/Availability of Report:	DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.
5. Name of Performing Organization:	Dean of Academics Office
6. Office Symbol: 1	7. Address: NAVAL WAR COLLEGE 686 CUSHING ROAD NEWPORT, RI 02841-1207
8. Title (Include Security Classification):	Infocentricity and Beyond: How the Intelligence Community Can Survive the Challenges of Emerging Technologies, Shrinking Budgets, and Growing Suspicions
9. Personal Authors:	Diane L. Mezzanotte
10. Type of Report: FINAL	11. Date of Report: April 2000
12. Page Count: 16 (plus reference pages)	4861 words
13. Supplementary Notation:	A paper submitted to the Dean of Academics, Naval War College, for the Intelligence Directors Award (DIA) essay competition. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.
14. Ten key words that relate to your paper:	SIGINT, intelligence, encryption, communications, COMINT, FISA, Information Operations, network-centric, CIA, NSA

15. Abstract:

Advanced communications technologies threaten the U.S. ability to provide signals intelligence reports to strategists and policymakers. Budget cuts in the intelligence community and growing suspicion among the public add to the community's challenges of the Information Age. The author suggests a drastic restructure of the Intelligence Community and the adoption of an "infocentric" approach to intelligence collection and dissemination.

16. Distribution / Availability of Abstract:	Unclassified ✓	Same As Rpt	DTIC Users
17. Abstract Security Classification:	UNCLASSIFIED		
18. Name of Responsible Individual:	Dean of Academics, Naval War College		
19. Telephone: 841-2245		20. Office Symbol: 1	

Summary

The centuries-old wisdom of Sun Tzu to "know the enemy and know yourself"[1] applies more than ever in the Information Age. Ironically, the U.S. ability to know its enemy is being threatened by some of the same technologies that helped to make it an economic and military superpower. The worldwide availability of advanced communications technologies such as fiber optics, digital encryption, and computer-to-computer communications threatens to deny access to information vital to the nation's security: specifically, signals intelligence (SIGINT) collected and analyzed by the National Security Agency (NSA).

At the same time, as U.S. military strategy incorporates high-tech concepts including digital warfare and network-centric theater operations, reliance on national-level intelligence organizations such as NSA to provide intelligence to the warfighter will be reduced, if not eventually eliminated. Add the fact that the Intelligence Community has been criticized for duplication of effort, inefficient and expensive operations, perceived infringement on personal freedoms, and several notable intelligence failures, and it becomes clear that the U.S. intelligence structure must undergo change.

The approach advocated herein is rather drastic:

- Drop SIGINT collection of all but the highest priority targets as defined by the National Security Strategy, focusing target development efforts on human sources and the growing abundance of open-source information.
- Transfer responsibility for tactical-use SIGINT to the military services.
- Push for change to surveillance laws in order to achieve a proper balance between protecting personal freedoms and protecting the nation's security.
- Dismantle existing national-level intelligence organizations and rebuild the Intelligence Community, using a framework that combines process- and results-driven alignments.
- Establish an "infocentric," forward-deployed approach to information analysis and dissemination to ensure more relevant, tailored intelligence.

Strong leadership, corporate visions, and an intense public relations campaign will be necessary to gain acceptance and ensure successful change, both within the Intelligence Community and among the U.S. public.

The Intelligence Community: Realigning to Fight the War After Last

The NSA Office of Corporate Relations presents daily, to visitors, an overview briefing of the agency's mission. In it, reference is made to the "challenges" that NSA faces at the start of a new millennium. The word "challenge" is accurate but understated: NSA is facing a serious survival problem, brought about by the widespread use of emerging communications technologies and public encryption keys, draconian budget cuts, and an increasingly negative public perception of NSA and its SIGINT operations.

NSA is not the only intelligence agency facing such challenges. Budget cuts and force reductions are affecting the Central Intelligence Agency (CIA), the Defense Intelligence Agency (DIA), and most other agencies. The Intelligence Community (IC) as a whole is under scrutiny as Congress, the media, and the public question the continued need for a massive intelligence structure in an era of relative peace.

In the last several years, CIA, DIA, and NSA all have undergone internal change in response to external drivers. At NSA, personnel strength has been reduced by one-third since the end of the Cold War[2] and the Directorate of Operations, in which the bulk of the SIGINT mission is conducted, has seen four major reorganizations in 10 years. NSA's latest initiative, christened "100 Days of Change" by current Director Lt. Gen. Michael V. Hayden, has gained national media attention.

Despite these attempts at improvement within NSA and other intelligence agencies, the overall intelligence structure is arguably no more effective or efficient than 10 years ago. One

could even argue that things have gotten worse: for every intelligence success such as the achievement of information superiority in Desert Storm[3], there is an embarrassing and potentially dangerous intelligence failure. The IC's failure to predict the 1998 Indian nuclear test and the erroneous bombing of the Chinese embassy in Belgrade are prime examples. Perhaps the problem lies in the fact that the transformation of the Intelligence Community is being approached in piecemeal fashion. Each agency is being asked to make internal changes, while the IC's overall structure and the functions of each member agency remain unchanged.

What is needed is a revamp of the overall IC force structure. While the military focuses its strategic force plans on winning the war after *next*, the IC can't seem to let go of the force structure that won the war after *last*: the Cold War. The IC should follow the military's lead and plan an intelligence force able to respond to the informational needs of both the tactician and the strategist 20 years hence: the informational war after next. Such a force would most likely look drastically different than the IC of today, and would require a massive transformation—one that goes beyond in-house changes and redefines the role of and relationships among IC organizations.

Three major problems facing the IC today must be addressed within force planning or they will continue to worsen: the diminishing ability to collect and analyze signals intelligence; dwindling resources and inter-agency redundancies; and a growing negative perception of the U.S. Intelligence Community as "Big Brother." These issues are closely related to each other: communications advancements mean that more money and resources will be needed to provide SIGINT support to military and political planners, but will Congress and the American public approve of increased funding to an area of government whose actions fall under suspicion?

Background: The Three Branches of SIGINT

In 1952, just after the start of what we now know as the Cold War, the National Security Agency (NSA) was created to provide signals intelligence, or SIGINT, in support of U.S. and allied military commanders, national-level policymakers, and political strategists. Most often associated with cryptology (the making and breaking of codes), SIGINT is actually broader in scope. It consists of three elements: communications intelligence (COMINT), electronics intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT).

- COMINT is based on the *contents* of communications signals: phone calls, faxes, teleprinter messages, e-mails, HF radio conversations, etc. COMINT can shed light on subjects such as the chain of command within a foreign military organization, political developments within another country, or the voting intentions of a foreign ambassador to the United Nations.
- ELINT derives information from the *signal parameters* emitted by aircraft, weapons systems, and other platforms. ELINT can help track the flight path of an aircraft, shed light on the operational command and control of a foreign weapons system, or indicate when a ground-based radar site is active (and where is it located)
- FISINT, like ELINT, derives information from *non-communications* signals, usually telemetry signals between components of a system. The IFF system (Identification, Friend or Foe) used in commercial and military aircraft is an example of a non-communications signal that carries valuable information.

In general (but not across the board) most strategic-level intelligence comes from COMINT, while FISINT and ELINT are used more in the tactical/operational realms.

Access Denied: Overcoming the Threat of Silence

For most of its existence, NSA enjoyed the luxury of easy access to foreign signals of national security importance to the United States. With the introduction of each new communications technology came the discovery of its vulnerability and a means of relatively passive collection. Reconnaissance aircraft or ground stations, flown or placed within range, easily collected high frequency (HF) communications. Microwave radio transmissions were

collected by satellites picking up signal "spillage" between relay stations. VHF radio, cellular phones, even undersea telephone cable communications all were accessible by passive collection means.[4] So until the 1990s, NSA's biggest task lay not in the *collection* of communications signals, but in their *exploitation*: decryption, demodulation and, often, translation into English were resource challenges, because it became impossible to process all the signals being collected.

Perhaps because NSA was focusing on how to solve that production bottleneck and on other internal issues, the agency failed to see the coming "cyberrevolution" and its impact on COMINT efforts until it was too late. Suddenly, traditional COMINT sources fell silent as the world turned to new and inexpensive methods of communicating: digital, encrypted communications and fiber optics technologies. Inexpensive and virtually impossible to crack, even by using supercomputers, these new methods have become the standard in the communications industry and have resulted in a global information network used by virtually everyone: embassies, foreign ministries, businesses, militaries, private individuals, terrorists…

The full impact on COMINT has yet to be realized, but it won't take long. In 1999, 90 percent of the world's communications were unencrypted, compared to just 10 percent encrypted communications. Before 2010, the statistics will have reversed: at least 85 percent of communications will be encrypted and—barring any revolution in decryption technologies—inaccessible to NSA and the IC.[5] As Hersh puts it, "the code-makers are leaving the code-breakers far behind."[6]

The "Selective Hearing" Solution

How does NSA continue to provide COMINT support to military and political strategists in the new communications environment? It can't—not by itself and not by using the usual high-

tech methods. One of the ironies of the communications revolution is that it will force intelligence methods to take five steps backwards and rely more on active collection techniques of the past: planting "bugs" in computer equipment, stealing passwords or encryption keys, infiltrating organizations. In order to continue to provide COMINT, the human intelligence (HUMINT) discipline must be expanded because the IC will be forced to beg, borrow, and steal in order to gain access to communications.

This type of active collection is associated more with the CIA than with NSA. Joint collection operations will increase, and perhaps even lead to a restructuring, discussed later. At the least, however, because collection will be more manpower intensive, high-risk, and expensive, a policy of "selective hearing" will have to be implemented. The communications of only those targets of highest interest to the U.S. in terms of security strategy will be "staked out" while other, lower-priority targets will be dropped. In other words, NSA and the IC will have to face the fact that COMINT just won't be available on all targets, as it was in the past, and that other methods of information analysis will have to be relied upon for targets of less strategic importance.

Redefining the Fourth Amendment for the Information Age

Computer-to-computer, or C2C, communications pose a different challenge. Technology already exists to collect passively data sent over the Internet. Currently, the United States serves as the hub for Internet communications: most of the world's Internet capacity lies in the United States and most Internet communications travel via servers located in the United States, regardless of origin.[7] Add to this the fact that Internet Protocol (IP) addresses identify the country and site of both the originator and the recipient, and in theory NSA should have easy

access to foreign Internet messages of national security interest without running much risk of inadvertently collecting private U.S. and Allied communications.

However, current policy, based on legal interpretation of the 1978 Foreign Intelligence Surveillance Act (FISA), prohibits the collection and exploitation of these U.S.-relayed Internet communications. FISA is a necessary law: enacted in the wake of intelligence abuses at the hands of a corrupt administration[8], it protects the Fourth Amendment rights of law-abiding U.S. citizens by ensuring that the government will not eavesdrop on their communications. And, contrary to recent media allegations[9], FISA is strictly adhered to by NSA and the IC, who are held accountable by oversight committees, the FISA court, and strict in-house measures of compliance.

FISA as it currently is written, however, makes it extremely difficult for the IC to conduct some operations of national security importance, such as counterintelligence investigations. Many point to overly restrictive FISA laws as the culprit in the Dr. Wen Ho Lee espionage situation: the Los Alamos scientist was suspected of espionage long before he passed nuclear weapons secrets to Taiwan, but was not under full surveillance because of FISA technicalities. The loss of those secrets, according to one witness at the bail hearing for the accused, could "change the global strategic balance"[10] and might not have occurred under a more permissive FISA.

FISA was written in the 1970s, long before anyone envisioned a global communications network such as the Internet. While it's easy to understand why an international phone conversation with one communicant in the United States should be protected under FISA, it seems counterproductive to U.S. security goals to extend the same blanket protection to an e-

mail sent from Seoul to Baghdad via a server at Harvard University. Members of the President's Foreign Intelligence Advisory Board have asserted that:

> [W]e do believe that the Department of Justice may be applying the FISA in a manner that is too restrictive, particularly in light of the evolution of a very sophisticated counterintelligence threat and the ongoing revolution in information systems.[11]

Clearly, it's time to redefine FISA to include a provision for the proper and legal collection of foreign entities' Internet communications that transit the United States. The biggest obstacle to such change, of course, would be convincing the American public (and members of Congress) that this collection privilege (a) is necessary to protect the nation's security and (b) would not be abused. Both could be accomplished through more open dialogue—an occasional, authorized release of classified information to show how FISA collection saved American lives, or media coverage of the strict measures NSA follows to protect privacy rights would go a long way in regaining trust and credibility. Remaining silent on the matter only fuels conspiracy theorists.

Doing More With Less: Building a Leaner, More Efficient IC

The proliferation of unbreakable communications is just one of the problems facing the IC. Continued pressures to cut back on inflated Cold War budgets and to reduce duplication and inefficient processes call for a smaller but more effective national-level intelligence force structure. One option would be to shift responsibilities for the more tactical-level SIGINT operations directly to the military, for better in-theater use. A more drastic—but more complete—option would be a total realignment of resources and responsibilities within the IC. Both might be necessary.

Transferring ELINT and FISINT Collection In-Theater

Under current organizational structure, most SIGINT support to military operations is conducted from NSA HQ in Fort Meade, Maryland. Signals are collected remotely and forwarded to NSA for processing and analysis, then the resulting intelligence information is disseminated worldwide to a variety of users at both the tactical and strategic level. While all three areas of SIGINT have both tactical and strategic uses, FISINT and ELINT generally are more tactical in nature—they are the disciplines that will be used in the digitized, sensor-heavy battlespace of the future. The informational battlespace "mesh" envisioned by Martin Libicki and others[12] relies on in-theater sensors such as unmanned aerial vehicles (UAVs), lightweight and low-orbiting satellites, and other automated methods of information technology to provide the soldier with the answers to three vital targeting questions (Where am I? Where are my buddies? Where is the enemy?[13]) and a low-risk means of precision firepower (through robot- or satellite-controlled weapons).

If the military services are, indeed, building a digitized force that fights techno-wars on a "meshed" sensor battlefield, then the reality is that NSA's involvement in FISINT and ELINT collection and dissemination would add an unnecessary layer and should be eliminated. By shifting responsibility for FISINT and ELINT to DIA and the military services, NSA would be better able to focus its resources on the COMINT challenges it faces, particularly those at the strategic level.

Rebuilding the IC Force Structure

Joint Vision 2010 recognizes that future military operations will be multi-service by nature and that traditional distinctions between service-specific operations are, in many cases, no longer relevant: the Air Force is not the only service that conducts airstrikes, and amphibious

landings are no longer the domain of just the Marines. Objective-based force planning also has helped to blur service-specific distinctions. Rather than asking, "How many infantry battalions should make up an Army division?" force planners are focusing more on the desired end result: "If we wanted to destroy the enemy's military center of gravity, what would we need and how would we do it?" The military structure, in other words, is taking a holistic, objective-oriented approach to force planning.

Meanwhile, the Intelligence Community continues to operate as a collection of separate, monolithic, and often competing, agencies. First, there is the distinction between intelligence producers and intelligence users. Of the 13-member IC[14], most are strictly *users* of intelligence, while the four major intelligence *producers* are CIA, DIA, NSA, and the National Imagery and Mapping Agency (NIMA). A second-level distinction occurs among the intelligence producers; each is defined by the types of information it collects, analyzes, and produces:

- CIA produces HUMINT, or intelligence derived from human sources (agents, spies).
- DIA produces MASINT: Measures and Signatures Intelligence, which gleans information from metrics such as satellite footprints or acoustic patterns.
- NIMA produces imagery intelligence, or IMINT, based on various types of satellite images: photographic, infrared, multispectral, etc.
- NSA produces SIGINT, or intelligence derived from foreign electromagnetic signals.

So, the U.S. intelligence-producing organizations currently are aligned according to information source. This approach worked well for the duration of the Cold War, but is no longer as effective or workable today, for several reasons:

- The lines between "INTs" have blurred. When a foreign embassy spokesman prepares a press release and forwards it to the media via e-mail, is that considered a SIGINT source, a HUMINT source, or an open-source record?
- Target expertise is too compartmented to be effective. CIA, DIA, NSA, and others all have in-house experts on particular regions or topics—China, Iraq, weapons

proliferation, narcotics trafficking—but the "separate and unequal" IC culture built during the Cold War discourages interaction and collaboration. The result: duplication of effort, piecemeal conclusions, and intelligence failures.

- Gaining access to one "INT" is going to become dependent on one or more other "INT"s. For instance, Allied forces were able to record conversations off the mobile telephone system Saddam Hussein used during the Gulf War, but not through the usual methods of using an NSA supercomputer to isolate, demodulate, and decrypt the voice signal. Rather, a CIA-recruited agent provided the phone system's technical manuals and other data that allowed access to the signal.[15] Joint intelligence operations, therefore, will become the rule rather than the exception, but the current structure is not conducive to jointness.

Another aspect to consider is that the IC's current reliance on "special source" intelligence such as the "INTs" already described is expensive and, arguably, duplicative and unnecessary. Robert Steele, founder of Open Source Solutions, maintains that:

> [N]early 80 percent of the information the government considers classified is available to anyone for the asking...[T]he intelligence community could do a much better job for less money, and with less danger, if it spent its energies on collecting open-source information and turning that information into knowledge."[16]

How, then, does the IC reinvent itself to overcome the challenges of duplication, expense, disappearing "special" sources and emerging open sources? Two options would be to realign based on process or by objective.

The Intelligence Cycle Blueprint

Aligning the IC parallel to the steps of the intelligence production cycles used at every agency—i.e., a process-based structure—seems to be a viable option. The SIGINT cycle, for instance, consists of four basic steps: requirements, access, exploitation/analysis, and dissemination. First, a customer (State Dept., CENTCOM, etc.) levies a requirement for information on a particular subject: say, the Iraqi Revolutionary Guard's order of battle. Signals which might carry information satisfying that requirement are identified and, with any luck, access is gained. Once the signal is collected, a great deal of processing usually is required:

demodulation, isolation of a voice signal, decryption of printer traffic, translation from a foreign language into English, and analysis of the information. The resulting intelligence analysis findings are disseminated to the customer(s) who originated the requirement and to others in the IC with a need to know the information; this usually occurs in the form of a SIGINT report.

While the cycle just described is the SIGINT cycle, virtually any intelligence production cycle could be described with the same four basic steps. Using a process-aligned structure based on the intelligence cycle, then, four organizations would be appropriate:

- A *requirements staff* to gather, disseminate, and track intelligence requirements across the IC. Currently, separate interagency committees establish priorities for each discipline (SIGINT, HUMINT, etc.), resulting in lengthy bureaucratic processes and conflicting viewpoints. Establishing a neutral organization to streamline the process and oversee a largely automated accountability/tracking mechanism would improve overall operations and reduce operating costs for this step of the cycle.
- An *access agency* tasked with gaining access to information. Access operations would be both defensive (tasking a HUMINT case officer with developing more in-country sources or moving a satellite 20 degrees northward to target a communications signal) and offensive (disrupting an enemy's C3 network) in nature. This agency would require a technology-savvy workforce to face some of the access challenges already discussed.
- An *all-source research and analysis agency* to develop an in-depth knowledge base on topics vital to the U.S. national security. Target experts currently split among CIA, DIA, and NSA would be combined into a smaller, smarter, and less duplicative IC analytic workforce than the existing one.
- An *information assurance agency* to maintain a secure, reliable (and bandwidth-heavy) network connecting all members of the IC. This network would allow automated dissemination of intelligence estimates and reports.

The IO Objective Model

An alternate approach would be to build intelligence forces around information operations (IO) capabilities needed to meet national security goals. Some capability examples:

- Precision strike against enemy communications: destroying a particular communications satellite, blocking access to a Web site, or cutting a fiber optics cable.

- Strategic bombing of enemy centers of gravity: shutting down an entire power grid or a command-and-control network using weapons of "mass disruption" such as computer viruses.
- Intelligence, surveillance, and reconnaissance (ISR) operations for U.S. forces: tactical ISR (the automated, digitized battlespace) and in-depth analysis for strategists (insight into the human aspect of a particular enemy's politics and warfare).
- "Lift" and rapid deployment: placing sensors, networks, and power supplies in theater; "deploying" analytic assets against new targets in support of crises.
- Logistical support: protecting U.S. information systems security (INFOSEC) and ensuring a reliable C4I infrastructure.

A Hybrid Approach

Restructuring the IC around capabilities would require an intelligence force of considerable *depth*: information technology specialists and topical/cultural experts. A process alignment would place more emphasis on *breadth* and would fit with the current move to produce multi-disciplined analysts who can be moved from target to target in response to world events. The IO model fits more closely with military strategy and force structure, while the process model is more closely tied to the current IC structure and would probably be less difficult to implement. Both models have pros and cons; perhaps the most obvious approach is to re-establish intelligence organizations based on process and then develop specialized, IO-focused units within those organizations.

In any case, such restructuring would standardize operations, centralize and expand target awareness and IO capabilities, and reduce operating costs. The new force structure could accomplish "more with less"—a current mantra among IC budget managers.

Building a Forward-Deployed, Infocentric Intelligence Community

Regardless of the model used to realign or rebuild the IC, an important goal would be to transform the mounds of information available to the IC into usable and useful knowledge. For

information to be transformed into knowledge, it must be relevant to the mission needs of specific organizations. This is another area in which the IC currently falls short, and would do well to heed the example of the military services.

The presence of J2 intelligence staffs within the military commands allows for the selection, tailored analysis, and effective use of intelligence in theater. A similar approach could be taken among non-military members of the Intelligence Community. Intelligence staffs tuned in to the particular informational needs of their host agencies would be part of an information-sharing network. They would, in effect, serve as forward-deployed units of the all-source intelligence analysis agency used in both models above. A similar approach is advocated by Steele, who advocates an intelligence network in which "instead of giant pools of analysts working in a central agency, many will be reassigned to work inside governmental departments like Commerce, Treasury, State, or Agriculture...tailoring analysis on the spot to the needs of the users."[17]

Building on the concept of network-centric operations used in the business world and in war plans, the IC could create an effective network-centric method of intelligence analysis and dissemination. An informational "mesh" and "net" operation is used by companies such as Wal-Mart[18] to turn tactical point-of-sale information ("How many lightbulbs were bought in Duluth today?") into strategic production planning ("We will need to manufacture and ship five cases of lightbulbs to Duluth before next week."). Similarly, the New York City Police Department has reduced serious crime by using a network-centric approach that combines policemen's in-depth knowledge of a specific "beat" with networked information on citywide crime data. [19] In both cases, piecemeal tactical information becomes strategic knowledge through tailored analysis.

An IC comprising small, specialized teams (target experts) and connected by an information-sharing network could achieve similar success. Forward-deployed intelligence staffs at specific agencies could tap into the information network and build a knowledge base with which to make sound, informed tactical and strategic decisions. The line between intelligence user and intelligence producer would blur as all IC members contribute to and draw upon that network. This approach could be called an "infocentric" approach to intelligence.

The first steps to creating an infocentric IC were taken a few years ago by the Unified Cryptologic Architecture 2010 (UCA 2010), an interagency working group tasked with identifying challenges faced by the IC in the next 10 years. Efforts to modernize and standardize the IC with state-of-the-art, compatible analytic workstations and communications systems already have begun. The groundwork has been laid for an infocentric intelligence force.

Knowing the Enemy Within: Leadership Challenges Posed by Drastic IC Changes

These proposed changes to the IC are drastic ones that transcend organizational, policy, and cultural changes. Incorporating them would inflict a substantial period of confusion, resistance, and pain on the IC workforce. Just as NSA's director acknowledges that it's time to sacrifice some degree of readiness in an effort to modernize[20], the long-term payoff for short-term sacrifices would be a new, improved IC—one better able to "mine" information and turn it into knowledge useful to national security strategists.

Regardless of the approach taken to streamline U.S. intelligence operations, strong, dedicated, and trusted leadership will be needed. A corporate approach will be necessary. Several goals will have to be met:

- The Intelligence Community itself will have to embrace the idea of change. The severity of the current situation must be realized: the IC must change or be run out of business by the information technology sector of private industry.

- The strategic plan to build an improved IC must be communicated clearly to its members, who must understand why they are being asked to change before they agree to change. A restructured IC would require some employees to change job locations, learn new skills, or undergo some other type of major change, all of which will require "buy-in" from the workforce.
- Leaders must be prepared to deal with morale problems arising from cultural clashes. Decades-old rivalries between CIA and NSA, for instance, have resulted in strong opinions and social class-like structures and attitudes that would come to a head when and if the two workforces were ever combined.
- A public relations campaign will be necessary to gain public acceptance of policy changes and Congressional approval of funding for an IC revitalization.

Of the above goals, the last one probably is the most important. For decades, U.S. intelligence agents have been portrayed negatively in movies, novels, and in the press. Almost 50 years of steadfast silence on the nature of NSA operations, while necessary during the Cold War, are coming back to haunt NSA in the form of bad press and public suspicion. The CIA constantly makes headlines for perceived failures or abuses. The general public is, more or less, unaware of DIA's existence or its role in the nation's security. Before taxpayers and Congress approve continued funding for the IC, they first must understand why such an institution is necessary.

And an intelligence structure is, indeed, necessary in today's era of transnational threats and uncertain foes. Just how that structure looks and what role it plays are the variables which must now be redefined. In order to fight the Third Wave wars described by the Tofflers in their famous book War and Anti-War,

> "Either intelligence itself assumes a Third Wave form, meaning it reflects the new role of information, communication, and knowledge in society, or it becomes costly, irrelevant, or dangerously misleading." [21]

To paraphrase Hayden: by standing still, NSA and the Intelligence Community have fallen dreadfully behind.[22] Catching up is possible, but will require drastic measures aimed at the ultimate objective: maintaining an edge in informational awareness of potential enemies in order to ensure the security of the United States and its citizens.

[1] The full quote is, "If you know the enemy and know yourself, you need not fear the result of a hundred battles." Sun Tzu, The Art of War 4th century B.C.: available online at Bragi.com http://www.bragi.com/classics/t/st-300/index.shtml, Copyright 1999-2000: Section III, "Attack by Strategem."

[2] Gregory Vistica and Evan Thomas, "Hard of Hearing," Newsweek 13 December 1999: Downloaded from http://cryptome.org/nsa-sees.htm, 27 Jan. 2000.

[3] According to the official NSA overview briefing, presented on a regular basis by the Office of Corporate Relations, Desert Storm marked the first time information superiority was achieved on the battlefield: U.S. and Allied forces enjoyed an uninterrupted flow of communications while being able to exploit and/or disrupt Iraqi communications.

[4] Information on collection methods is from Duncan Campbell's Development of Surveillance Technology and Risk of Abuse of Economic Information (Vol. 2/5) (Luxembourg: October 1999): 4; Downloaded 20 February 2000 from http://cryptome.org/dst-pa.htm.

[5] These encryption statistics (which are unclassified) are cited in various in-house briefings presented by NSA's Director and his Office of Corporate Relations. The briefings themselves currently are classified and not available to the public.

[6] Seymour M. Hersh, "The Intelligence Gap," The *New Yorker* 6 December 1999: 60.

[7] Campbell 10.

[8] During the Vietnam War and with approval of the Nixon administration, SIGINT resources were used to collect the communications of U.S. citizens who protested the war. A detailed account of such operations can be found in U.S. Senate, Select Committee to Student Governmental Operations With Respect to Intelligence Activities, Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans (Washington, GPO, 1976).

[9] Media reports on the ECHELON intelligence collection system has led to widespread speculation that NSA spies on private U.S. communications.

[10] Testimony was from Dr. Stephen Younger, assistant laboratory director at Los Alamos, December 13, 1999. Quoted in U.S. Senate Bill 2089, introduced on the floor 24 Feb. 2000 and cited online. (Congressional Record Online, http://www.access.gpo.gov/su_docs/aces/aaces002.html). The bill seeks more leniency in granting FISA exceptions to counterespionage investigations and other situations of national security importance.

[11] U.S. Senate, A Special Investigative Panel of the President's Foreign Intelligence Advisory Board, Security at its Worst: A Report on Security Problems at the U.S. Dept. of Energy (Washington, GPO: June 1999). Presented at an open meeting of the Senate Committee on Armed Services, June 22, 1999 and available online at http://www.nsa.gov/about_nsa/mission.html.

[12] See, for instance, Martin C. Libicki's The Mesh and the Net, Washington: NDU, 1995), p. 31ff; the descriptions of Third Wave warfare in the Tofflers' War and Anti-War (New York: 1995); and the visions of future warfare described in the essays edited by Robert Bateman, III in Digital War Novato, CA: Presidio Press, 1999).

[13] Robert Leonhard, "A Culture of Velocity," in Digital War.

[14] The Intelligence Community consists of the: CIA, DIA, Dept. of Energy, FBI, National Imagery and Mapping Agency (NIMA), National Reconnaissance Office (NRO), NSA, State Department's Bureau of Intelligence and Research, Dept. of the Treasury, and intelligence arms of each of the armed services: Air Force, Army, Navy, and Marines.

[15] Hersh 58.

[16] Winn Schwartua, Information Warfare: Chaos on the Electronic Superhighway (New York: Thunder Mouth Press: 1994) 339.

[17] Steele as quoted by the Tofflers, 190.

[18] VADM Arthur K. Cebrowski, USN and John J. Garstka, "Network-Centric Warfare—Its Origin and Future," U.S. Naval Institute Proceedings, January 1998, pp. 30-31.

[19] Cebrowski and Garstka, 34.

[20] Lt. Gen. Hayden has cited this concept many times in press statements and in communiques to the NSA workforce since the November 1999 start of "100 Days of Change."

[21] Tofflers 181.

[22] Hayden as quoted by Vistica and Thomas.

Bibliography

Bateman, Robert L., ed. Digital War: A View from the Front Lines. Novato, CA: Presidio Press, 1999.

Campbell, Duncan. Development of Surveillance Technology and Risk of Abuse of Economic Information. (Vol. 2/5) *Report to the General Directorate for Research of the European Parliament's Scientific and Technical Options Assessment (STOA) program office*. Luxembourg: October 1999. Downloaded 20 February 2000 from *http://cryptome.org/dst-pa.htm*.

Cebrowski, Arthur K. VADM, USN, and John J. Garstka. "Network-Centric Warfare—Its Origin and Future," U.S. Naval Institute Proceedings. January 1998.

Colangelo, Philip. "The Secret FISA Court: Rubber Stamping on Rights," Covert Action Quarterly, online. Downloaded 20 February 2000 from http://mediafilter.org/caq/Caq53.court.html.

Hayden, Michael V., Lt. Col., USAF. Address to Kennedy Political Union of American University, 17 February 2000. Downloaded 28 February 2000 from *http://www.nsa.gov/releases/dir021700.html*.

_____. Address to the House Permanent Select Committee on Intelligence, February 29, 2000. Forwarded in unclassified, internal e-mail to the NSA workforce, March 2, 2000.

Hersh, Seymour M. "The Intelligence Gap," New Yorker. December 6, 1999.

Johnson, Stuart E. and Martin C. Libicki, eds. Dominant Battlespace Knowledge: The Winning Edge. Washington, DC: National Defense University, 1995.

Krizan, Lisa. Intelligence Essentials for Everyone. Washington, DC: Joint Military Intelligence College, 1999.

Libicki, Martin C. The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon. Washington, DC: National Defense University, 1995.

_____. What is Information Warfare? Washington, DC: National Defense University, 1995.

The National Security Agency's homepage on the Internet: *http://www.nsa.gov/about_nsa/mission.html*

The President's Foreign Intelligence Advisory Board. Security at its Worst: A Report on Security Problems at the U.S. Dept. of Energy. Washington: GPO, 1999. Presented at an open meeting of the Senate Committee on Armed Services, June 22, 1999. Downloaded 9 April 2000 from *http://www.nsa/gov/about_nsa/mission.html.*

Risen, James. "A Top-Secret Agency Comes Under Scrutiny and May Have to Adjust," The New York Times, online. December 5, 1999. Downloaded 27 January 2000 from *http://www.nytimes.com/library/review/120599security-agency-review.html.*

Schwartau, Winn. Information Warfare: Chaos on the Electronic Superhighway. New York: Thunder's Mouth Press, 1994.

Specter, Arlen. "Statement on Senate Bill 2089, Bill to Amend the Foreign Intelligence Surveillance Act of 1978." *Congressional Record:* February 24, 2000. From the Congressional Record Online via GPO Access [*wais.access.gpo.gov*], downloaded 28 February 2000.

Strobel, Warren P. "The Sound of Silence?" U.S. News & World Report. February 14, 2000. Downloaded January 27, 2000 from *http://cryptome.org/nsa-sees.htm.*

Toffler, Alvin and Heidi. *War and Anti-War*. New York: Warner, 1995.

U.S. Senate. Statements on Introduced Bills and Joint Resolution [excerpt]. Senate Bill 2089, a bill to amend the Foreign Intelligence Surveillance Act of 1978. Congressional Record Online: February 24, 2000. *http://www.access.gpo.gov/su_docs/aces002.html*

U.S. Senate, Select Committee to Student Governmental Operations With Respect to Intelligence Activities. Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans. Washington, GPO: 1976.